

# NFC -Forensisk bildanalys

2018-05-24

# Undersökningar: Forensisk Bildanalys

- Bildjämförelse
- Återskapa bild, video och ljud
- Äkthetsundersökning av bild och video
- Kameraidentifiering
- Övrig bild- och videoundersökning
  - Händelseförlopp
  - Tidsbestämning
  - Teknisk analys
  - mm

# Framtida utmaningar

- Nästan alltid omkomprimerat vid uppladdning på nätet
- Avsiktlig manipulation av metadata eller metadata försvinner vid uppladdning på nätet
- Användning av **appar** vid filmning och fotografering
- Användning av bildstabilisatorer försvårar Kamera-ID
- AI-genererade filmer/bilder (ex. DeepFake)
- Brist på bra verktyg för analys av äkthet i video
- Bättre kameror har möjliggjort jämförelse av objekt som ej tidigare varit möjliga att analysera/jämföra
  - Behövs mer forskning inom vissa områden
  - Omöjligt att ha exakt statistik
  - Okunskap inom rättsväsendet
- Klustring av större mängder av bildmaterial av kamera-sensorbrus tar lång tid

Återskapande av bild- och  
videomaterial

# Återskapande av bild- och videomaterial

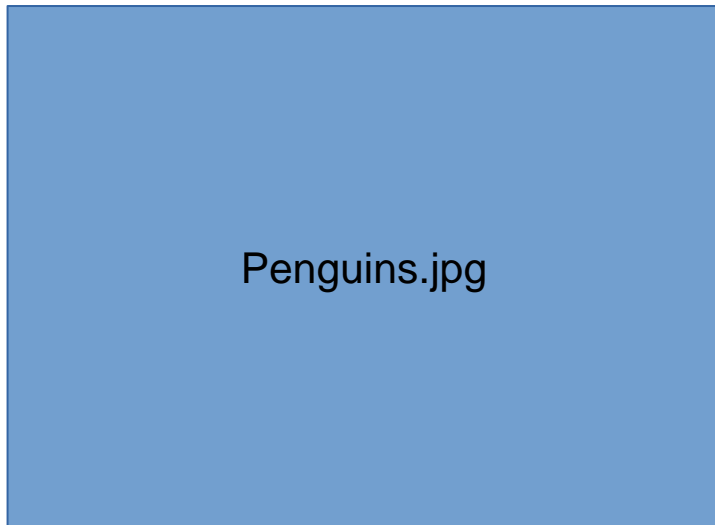
- Görs då lagringsmedia är skadade, raderade eller på annat sätt inte läsbara
- Med utgångspunkt i de data som går att extrahera är målet att skapa spelbara/visningsbara mediafiler
- Stillbildaformat (t ex PNG, JPEG) kan i stor utsträckning hanteras med automatiska verktyg, medan video ofta kräver specialiserade implementationer pga filstorlek, fragmentering och speciella videoformat.
- Områden inom vilka utveckling bedrivs är till exempel automatisk validering av återskapad video och automatisk identifiering av kodningsparametrar

# Utmaningar

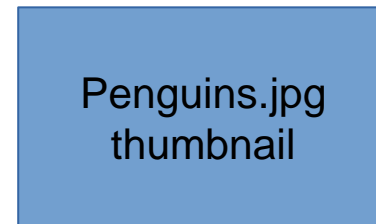
- Datamängder
  - *diskar i TB-storlek blir allt vanligare*
- Nya filtyper/kodekar
  - *t ex H.265/HEVC och nya kontainervarianter*
- Kryptering
  - *BF-metoder inte aktuella ("enkel" AES-ECB ~10<sup>19</sup> år)*
  - *lösningar bygger på svagheter och säkerhetsbrister*
- "Exotiska" filsystem och proprietära format
  - *helt ny implementation kan krävas för att läsa data*

# Uppgift: Carving av JPEG-thumbnail

*Penguins.jpg (exempelbild i Windows)*



...innehåller en annan JPEG-bild  
på adressintervall [359, 4653] (dec)...



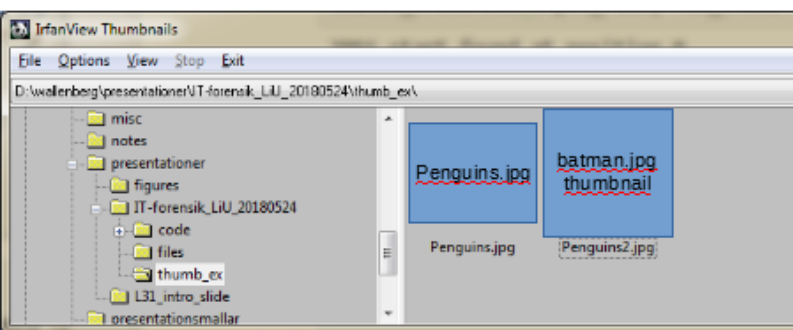
...en thumbnail som ligger i  
bildens Exif-data

*Hur kan man extrahera sådana thumbnails med hjälp av  
endast start-och slutmarkörer för JPEG-bilder?*

# Uppgift: Modifikation av JPEG-thumbnail

(extrauppgift, valfritt)

*När vi hittat vår thumbnail,  
hur kan vi byta ut den?*



**Ledtråd:** det är inte bara bildinformationen som måste ändras, utan även storleksangivelserna för thumbnail och Exif-data.

Söksträngarna

`\xFF\xE1`

och

`\x04\x00\x00\x00\x01\x00\x00`

kan vara användbara...

Penguins2.jpg